**STUDENT EXAMINATION VERIFICATION SYSTEM USING PHYSIOLOGICAL BIOMETRICS**

**BY**

**SOBOLA ABDULKAREEM ADEBARE**

**S121202031**

**A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, COLLEGE OF INFORMATION AND COMMUNICATION TECHNOLOGY, CRESCENT UNIVERSITY ABEOKUTA**

**IN PARTIAL FUFILLMENT OF THE REQUIREMENT FOR THE AWARD OF BACHELOR OF SCIENCE (B.Sc) DEGREE IN COMPUTER SCIENCE**

**SECTION ONE**

**INTRODUCTION**

* 1. **Background to the study**

Using Biometric features of a person for recognition/verification is becoming a common occurrence. Even though there are numbers of ways to prove authentication and authorization, biometric authentication beats all the techniques.In traditional method, a person desired to be identified submits an identify claim to the system via a magnetic strips cards, identity cards etc. All of these techniques suffer from common problems of inability to differentiate between an authorized person and an imposter who fraudulently acquires the access privilege of the authorized person. Biometric system is genuine and the identity of the person is dependent upon his/her physiological or behaviour attributes that can only identify a specific.

The biometric based exam hall authentication is to assist in the elimination of examination malpractice.Based on the usage of the number of traits, they divided as unimodal biometrics and multibiometric. Fingerprint is one of the easily accessible parts of the user and requires minimum efforts on the part of the user. Face detection is also included as it is, yet another option for human identification and authentication technology is also included, due to its high precision, as they are unique to each individual.

Biometric identification refers to identifying a specific individual to authenticate their identity, this technology can measure the physiological (e.g., Fingerprints, Vein, Patterns, Iris, Retina and the shape of the hand) and behavioral traits (e.g., Voice recognition, Gait, Gestures, The sound of the steps, and signature). A combination of characteristics can also be made as a multi-modal biometric, which improves measurement confidence. Such combinations could be face and fingerprint, face and iris, etc. The main benefit of biometric technology is that it collects unique human characteristics of each person (Thales,2020).

Humans normally identify between persons using their faces, and recent advances in computer vision capacity have enabled similar recognition to be made automatically (Ometov et al, 2019). Face recognition algorithms used simple geometric models in the past, but they have evolved into a science of complex mathematical models and representations throughout time, putting face and speech recognition in the spotlight for verification and identification (Sharma et al, 2021). The practice of comparing one biometric pattern to another to determine whether it should be rejected or accepted is known as verification.

**1.2 Statement of the problem**

In many educational institution, ensuring the integrity and authenticity of examinations has become increasingly challenging, methods of student identification, such as ID cards or signatures, are prone to errors, manipulation, and impersonation. This raises concerns about the legitimacy of exam results, as unauthorized individuals may take exams on behalf of others.

The growing reliance on online and remote examinations further complicates the issue, as physical supervision is limited. Therefore, there is a need for a reliable, secure, and efficient method to verify the identity of students during examinations. Physiological biometric, such as fingerprint scanning, facial recognition, or iris scans, present a potential solution to the problem.

**1.3Aim of the study**

The main aim of this study is to describe the student examination verification system using Biometrics.

**1.3.1 Objective of the study**

The general objective of the study is to:

1. access the accuracy and reliability of these biometric systems in ensuring that the person taking the examination is the correct student, thereby reducing the risk of impersonation and fraud;
2. explore the student and institutional perspectives on the adoption of biometric identification, including concerns related to privacy, consent, and potential technical challenges;
3. examine the feasibility of implementing biometric system in different educational settings, considering cost, infrastructure requirement, and scalability.

**SECTION TWO**

**LITERATURE REVIEW**

**2.1 Biometrics Technology**

Biometric can be defined as the physical or behavioural characteristics that can be used to digitally identify a person to grant him/her access to the systems.Typical examples of these biometrics identifiers include the following: fingerprints, facial patterns, voice or typing cadence Each of these identifiers is considered special to the individual and can be used in conjunction to ensure greater identity accuracy (Korolov, 2019).

Biometrics can be of two main kinds: physiological and behavioural biometrics. Each type relies on different traits and offers distinct advantages and challenges.

Biometric technology is widely used for two primary purposes: identification and access control (Ahmed,2019).

**2.1.1 Physiological Biometrics**

Physiological biometrics refers to physical attributes of an individual that are inherent and relatively stable over time. These characteristics are directly linked to the physical body and can often be captured using specialized sensors or imaging technologies. Most widely used physiological biometrics include:

1. **Fingerprint Recognition**

This is the most commonly used type of recognition system. It has been used in numerous applications for the past many years. It works on the unique patterns of ridges and valleys on the surface of a person’s fingers (Dargan et al,2020).

Each person’s fingerprints are distinct, even among identical twins, and they remain stable till person is alive. This type of recognition system records the minutiae (points where ridges end or bifurcate) and use these features to match against stored templates (Socheat et al,2020).

1. **Facial Recognition**

This recognition system makes the recognition of a person by using the unique features of an individual's face . Key features analyzed include the gap between eyes, nose shape, jawline, and the overall structure of the face. Modern facial recognition systems use deep learning algorithms to capture and match these features from images or videos (Kortli et al,2020).

1. **Iris Recognition**

The coloured part of a person eye is used in this system for recognition. Each person has unique patterns of the iris. It captures high-resolution images of the iris to identify distinctive features such as texture, colour, and patterns (Lee et al,2022). The iris is stable over a person’s lifetime and is difficult to alter or forge, making it a reliable method of biometric identification. Iris recognition is commonly used in high-security areas like airports and government buildings (Bharat & Shamily,2020).

1. **Voice Recognition (Physiological Aspect)**

Voice recognition systems analyse the physical aspects of a person’s voice, including pitch, tone, cadence, and the shape of the vocal tract (Li et al, 2019). Although voice recognition is influenced by factors like emotion and health, certain traits remain stable enough to offer reliable identification. Voice-based authentication is often used in mobile devices and call centers (Wang et al, 2020).

**2.1.2 Behavioral Biometrics**

Behavioral biometrics refer to patterns in the way people act or interact with their environment. Unlike physiological biometrics, which rely on physical traits, behavioural biometrics are dynamic and can change over time depending on context, mood, or physical condition. However, they can provide valuable data for continuous authentication in many applications. Some of the key types of behavioural biometrics include:

1. **Keystroke Dynamics**

In this type of biometric recognition system, the pattern in which a person uses a keyboard for typing is used for recognition. This includes factors such as typing speed, rhythm, pressure on keys, and the time spent between keystrokes (dwell time). Each individual develops a unique typing pattern, which can be used to authenticate them or detect fraudulent activity. Keystroke dynamics can be integrated into systems as a passive form of authentication, particularly in banking or online security applications (Porwik et al,2021).

1. **Speech Recognition**

While speech recognition also has a physiological component (voice), it has a significant behavioural aspect, as it involves how a person speaks rather than just what they say. Speech patterns, including cadence, accent, pitch, and even the rhythm of speech, can be unique to an individual. Continuous speech recognition systems can be used for identifying or verifying individuals in phone systems, voice-controlled assistants, and security applications (Isyanto et al,2020).

1. **Mouse Dynamics**

This recognition system uses the way a user interacts with a mouse or touch pad for recognition purpose. This includes speed, movement patterns, pressure, and click habits. Similar to keystroke dynamics, mouse dynamics can serve as a behavioural biometric to authenticate users or track unusual behaviour patterns in applications like online banking, e-commerce, and user verification systems (Khan et al,2024).

**2.2 Summary of Related works**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S/N** | **Author&Year** | **Method** | **Strength** | **Weakness** |
| **1** | Sarjiyus et al. (2023) | This authentication Technology uses  different biometric features, fingerprint, facial features and vein  pattern of the candidate  designed to eliminate impersonation. |  |  |
| **2** | Bhuiyan.M.A.,Samad.M.A., Hossain.M.S (2020) | The system uses deep learning algorithms for facial verification, consisting of two main stages: enrollment, where examinees register their facial data, and verification, where their identity is confirmed during the exam. | Deep-learning based methods have demonstrated state-of-the-art of high accuracy in facial recognition tasks. | The performance of deep learning models heavily relies on the quality and representatives of the training data |
| **3** | Singh.S.K., Yadav.A.K., Verma.R.K., (2019) | It proposes a framework that includes multi-factor authentication, encryption, access control, anonymization, and secure data storage. | The work presents new algorithm, encryption techniques and frameworks that offers enhanced security and privacy. | It lacks general applicability to all educational contexts. |
|  | Vaishnavi Kulkarni1, Mangita Waghmare2, Supriya Gund | This uses the fingerprint  identification to authenticate the identity of an individual. |  |  |
|  | Rajesh et al.(2020) | The system consists of a  fingerprint sensor connected to arduino microcontroller  circuit. In registration mode, the system allows to register up to 120 users and save their identity with respective id number. In addition it includes automatic iris recognition and palm vein technology. | It is the efficient and reliable  solution for stringent protection. |  |
| **1** | Jaimit Patel et al (2023) | It introduces a comprehensive frame  work for fingerprint recognition within system addressing the critical challenges like rotation, scaling  variations, noise, and distortions efficient in large datasets, accuracy, real-time performance, and reliability | The resultant  accuracy comes within the range of 89% to 99% across different conditions. | The accuracy reduces due to the lack of adaptability to noise. |
| **2** | Meennapa rukhiran et al (2023) | This study presents  the internet of things to develop flexible biometric recognition systems and an approach to assess the  quality of biometric systems for educational use. | The accuracy of the two-fingers multimodal  biometric system had the highest average of  96.67 percent. |  |
| **3** |  |  |  |  |

**SECTION THREE**

**METHODOLOGY**

The biometric based exam hall authentication is to assist in the examination malpractice and impersonation.Multi-biometrics system provides accuracy and can be established in much large scale biometric application.Fingerprint is one of the easily accessible parts of the user and requires minimum efforts on the part of the user. Face detection is also included as it is, yet another option for human identification and authentication technology is also included, due to its high precision, as they are unique to each individual.

Multimodal biometric authentication, which combines multiple biometric traits for identity verification, offers a more secure and reliable approach compared to single-modal authentication. Using both facial recognition and fingerprint recognition in examination verification is an effective way to reduce fraud, enhance security, and ensure accurate identity verification.

How it works:

1. **Facial Recognition**

**Capture**: During examination registration or entry, a live image of the examinee's face is captured using a camera.

**Processing:** The facial image is processed and compared to the stored facial data (previously registered during user on boarding).

**Verification:** The system checks the facial features like the distance between eyes, nose shape, and overall facial structure for a match.

1. **Fingerprint Recognition**

**Capture:** A fingerprint scanner is used to scan the user's fingerprints, usually at the time of entry or before starting an exam.

**Processing:** The scanned fingerprint is processed to extract unique features, such as ridge patterns, loops, and whorls.

**Verification:** The system compares the live fingerprint scan with the previously stored fingerprint template to confirm the examinee identity.

1. **Multi-modal Fusion**

**Authentication Process:** Both biometric traits (face and fingerprint) are combined for a higher level of security. The system checks for a match in both modalities, making it harder for unauthorized individuals to spoof or bypass the authentication process.

**Error Reduction:** In cases where one modality (e.g., facial recognition) may be less accurate due to poor lighting or positioning, the other modality (fingerprint recognition) serves as a reliable backup.

**Cross-validation:** The two systems work in parallel, enhancing the accuracy and reliability of the authentication process.

1. **Advantages for Examination Verification**

**Enhanced Security:** The combination of two biometric factors (something you are) reduces the likelihood of identity fraud, as it’s significantly harder to fake both a fingerprint and facial image.

**Non-intrusiveness:** Both methods are non-intrusive (no need for passwords or pins) and quick, ensuring minimal disruption to the exam process.

**Spoof Resistance:** Multi-modal systems are resistant to spoofing (e.g., using photographs or fake fingerprints) because a combination of features is required for successful authentication.

**Accuracy:** Combining the two modalities can improve overall accuracy, as errors from one biometric system can be cross-checked by the other.

**Online Exams:** For remote examination settings, students could use webcams for facial recognition and fingerprint scanners for secure log-ins.

**Physical Exams:** At exam centers, students can be verified at entry points with both facial and fingerprint scans.

**Proctoring:** During exams, biometric verification can prevent impersonation by verifying the student’s identity multiple times throughout the examination process.

**CHAPTER FOUR**

**CONCLUSION**

**Reference**

Saniya S. , Acharya P.P. , Sangeetha.A. , Sagarika.S. ., Priya.K. (2021) Multilevel Biometrics for Exam Hall Authentication.International Journal of Research in Engineering, Science and Management

Volume 4, Issue 5, May 2021 https://www.ijresm.com | ISSN (Online): 2581-5792

Bhuiyan.M.A., Samad.M.A., Hossain.M.S (2020) Biometric verification system using Facial Recognition.International journal of Computer Application(IJCA) Volume 176, Issue 1, September 2020 <https://ijcaonline.org> | ISSN(Online): 0975-8887

Tiwari.H.D., Tiwari.A.K., Kumar.V (2019) Iris Scanning Examination Verification System,International Journal of Computer Application Volume 178, Issue 1, July 2019 <https://ijcaonline.org> | ISSN(Online): 0975-8887

Singh.A.K., Shukla.K.K., Saha.S.C. (2020) Examination Verification Using Multimodal Biometrics,International Journal of Computer Applications Volume 176, Issue 4, August 2020 <https://ijcaonline.org> | ISSN(Online): 0975-8887

Singh.S.K., Yadav.A.K., Verma.R.K., (2019) Security and Privacy in Examination Verification System, International journal of Computer Application(IJCA) Volume 178, Issue 1, July 2019 <https://ijcaonline.org> | ISSN(Online): 0975-8887

Korolov, M, (2019) What is biometric? 10 physical and behavioural identifiers. CSO online. Retrieved 10 June 2020, from <https://www.csoonline.com/article/3339565/what>-is-biometrics-and-why-collecting-biometric-data-is-risky.HTML.

Ahmed, A.A. Future effects and impacts of biometrics integrations on everyday living. Al-Mustansiriyah J. Sci. 2019, 29, 139–144. [CrossRef]

Dargan, Shaveta, and Munish Kumar. "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities." Expert Systems with Applications 143 (2020): 113114.

Socheat, Sek, and Tianjiang Wang. "Fingerprint enhancement, minutiae extraction and matching techniques." Journal of Computer and Communications 8, no. 05 (2020): 55.

Kortli, Yassin, Maher Jridi, Ayman Al Falou, and Mohamed Atri. "Face recognition systems: A survey." Sensors 20, no. 2 (2020): 342.

Lee, Young Won, and Kang Ryoung Park. "Recent iris and ocular recognition methods in high-and lowresolution images: A survey." Mathematics 10, no. 12 (2022): 2063.

Bharathi, B., and P. Bindhu Shamily. "A review on iris recognition system for person

identification." International Journal of Computational Biology and Drug Design 13, no. 3 (2020): 316-331

Li, Xiaochang, and Mara Mills. "Vocal features: from voice identification to speech recognition by machine." Technology and culture 60, no. 2 (2019): S129-S160.

Wang, Chen, Yan Wang, Yingying Chen, Hongbo Liu, and Jian Liu. "User authentication on mobile devices: Approaches, threats and trends." Computer Networks 170 (2020): 107118

Porwik, Piotr, Rafal Doroz, and Tomasz Emanuel Wesolowski. "Dynamic keystroke pattern analysis and classifiers with competence for user recognition." Applied Soft Computing 99 (2021): 106902

Isyanto, Haris, Ajib Setyo Arifin, and Muhammad Suryanegara. "Performance of smart personal assistant applications based on speech recognition technology using IoT-based voice commands." In 2020

International conference on information and communication technology convergence (ICTC), pp. 640-645. IEEE, 2020

Khan, Simon, Charles Devlen, Michael Manno, and Daqing Hou. "Mouse dynamics behavioral biometrics: A survey." ACM Computing Surveys 56, no. 6 (2024): 1-33.

O. Sarjiyus, El Yakub M.B , Benjamin Ezra “Examination Verification System Using Biometric Authentication, International Journal of Integrative Sciences (IJIS) Vol.2, No.9, 2023: 1459-1478 (2023).

Rajesh N B, Subhiksha R, Oormila T S “BIOMETRIC EXAMHALL AUTHENTICATION” International Research Journal of Engineering and Technology (IRJET) Volume: 07 Issue: 04 | Apr 2020.

Jaimit Patel, Anubhav, Ayush Kumar Singh, Rachit Kumar Tiwari, Abhi Singh and

Bhupinder Kaur “Biometric Authentication System For Access Control” *School of Computer Science and Engineering , December 29-30, 2023.*

Meennapa Rukhiran , Sethapong Wong , and Paniti Netinant “IOT-BASED BIOMETRIC RECOGNITION SYSTEMS IN EDUCATION FOR IDENTITY VERIFICATION SERVICES: QUALITY ASSESSMENT APPROACH” College of Digital Information Technology, 9 March 2023.